Home Affairs Portfolio

Biometrics Strategy 2020–24

Australian Government
Department of Home Affairs

Australian
BORDER FORCE

AFP
AUSTRALIAN FEDERAL POLICE

AUSTRALIAN
CRIMINAL
INTELLIGENCE
COMMISSION

Australian Government
Australian Security
Intelligence Organisation

Australian Government
AUSTRAC

Home Affairs Portfolio

Biometrics Strategy 2020–24

CONTENTS

Foreword 4

Strategic context 6

- Why we need a strategy 6
- Strategy purpose 9

How and why we use biometrics 10

- What are biometrics? 10
- Why we use biometrics in the Home Affairs Portfolio 11
- Our Portfolio biometrics roles and capabilities 12

Our vision 15

Our approach 16

- Biometric data 17
- Community 18
- Our people 20
- Governance 21
- Systems 22
- Partnerships 24

What success looks like 26

Evaluating the Strategy 28

Appendices 30

- Appendix A: Home Affairs Portfolio privacy and ethics framework for the management of biometrics 31
- Appendix B: Biometrics roles by agency 34
- Appendix C: Portfolio agency biometric capability 39
- Appendix D: Strategic alignment 42
- Appendix E: Glossary 43

FOREWORD

The Home Affairs Portfolio brings together Australia's federal law enforcement, national security, transport security, criminal justice, emergency management, multicultural affairs, settlement services and immigration and border-related functions. While each agency is operationally independent, together we are responsible for significant biometrics capabilities and are custodians of valuable biometric data holdings.

This Portfolio Biometrics Strategy (the Strategy) articulates to our staff the importance of biometrics and strengthens the opportunities for joint agency activities.

It establishes a direction for a governance framework for our identity and biometric capabilities, and provides shared principles to guide future interoperability and capability alignment.

Michael Pezzullo AO
Secretary
Department of Home Affairs

Michael Outram APM
Commissioner
Australian Border Force

Reece Kershaw APM
Commissioner
Australian Federal Police

It sets out how and why we use biometrics and our approach to enhancing and sustaining not only the technology, but the skills enhancement of the people who design and use it, and investment in the quality and accuracy of the data that underpins it.

It is important that we build public confidence in the Portfolio as a trusted custodian of their personal information. This Strategy reinforces privacy principles and ethical standards to ensure that we exercise our powers lawfully and proportionately, and our actions are subject to full, appropriate scrutiny and independent oversight.

To achieve our vision, we will work collaboratively to develop fit for purpose identity and biometrics capabilities, including specialist skilled people to support our Portfolio's mission of a prosperous, secure and united Australia.

Michael Phelan APM
Chief Executive Officer
Australian Criminal
Intelligence Commission

Mike Burgess
Director-General of Security
Australian Security
Intelligence Organisation

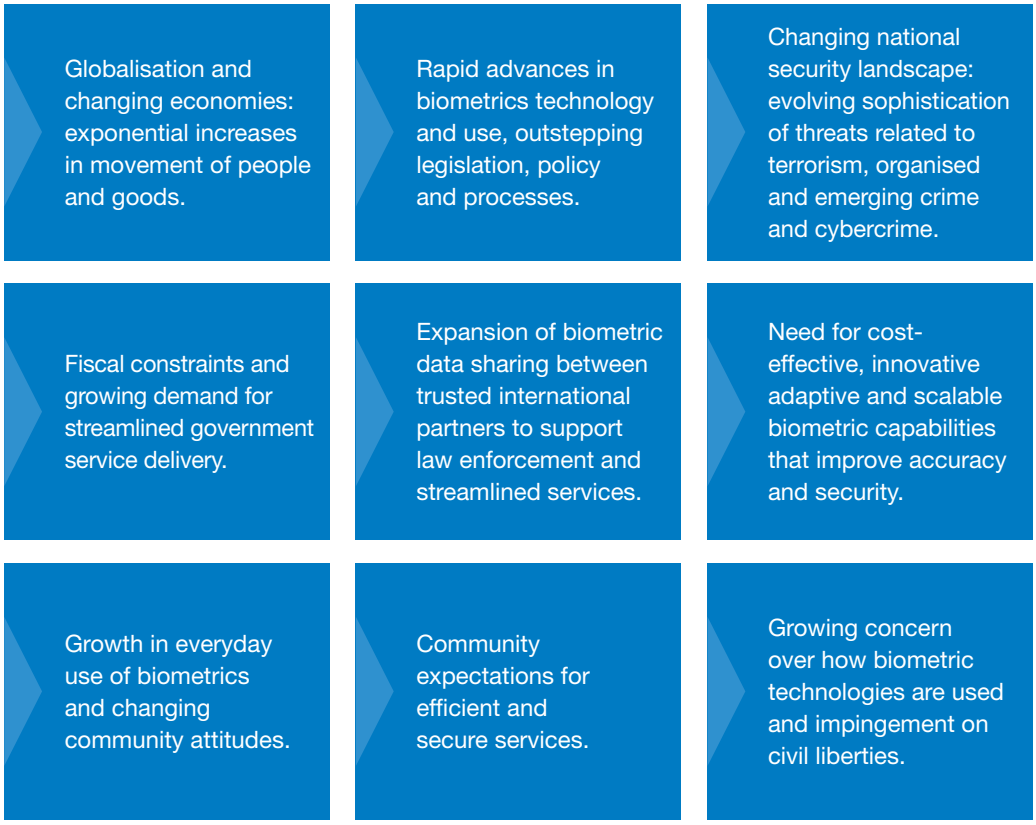
Nicole Rose PSM
Chief Executive Officer
Australian Transaction
Reports and Analysis Centre

STRATEGIC CONTEXT

Why we need a strategy

We operate in a dynamic geopolitical environment and must be prepared and equipped to address challenges resulting from: the increasing volume of travel and trade; the enhanced sophistication of methods used to break or exploit Australian laws; and the complexities of a more mainstream digitally connected world. As a Portfolio, and within a constrained fiscal environment, we also need to meet the public's expectations for convenient and simplified access to services by seeking innovation in our work practices.

Figure 1: Environmental context



The exponential growth of biometric technologies is also transforming the way the community carries out everyday activities. Australians already use biometrics to operate smart phones and computers and to access services such as banking and communications. Australians have also demonstrated that they are increasingly accepting of the government's use of personal identifiable information including biometric data, provided there is trust in its security and where the benefits of simpler service delivery are evident.[1]

Biometrics is a key and rapidly evolving capability and the Portfolio has invested significant financial and technical resources to develop these capabilities.

1. Personal identifiable information (PII) is any information that is used to prove or formally establish an individual's identity. PII includes biographical information (such as name, gender, date of birth and address) and biometric information (facial or vocal features, signatures, fingerprints, DNA, retina patterns and gait). Research indicates that Australians are increasingly willing to share their personal identifiable information if they understand why and how it is being used, and if they feel that they have some level of control over their data (Productivity Commission 2017, *Data Availability and Use*, Report No. 82, Canberra, pp. 169–189).

A strategy is required to harness opportunities offered by new and emerging technologies, to capitalise on technological advancements in biometric system accuracy, speed, the ability to identify risk, combat and disrupt crime and automate high-throughput and digital operations.

These technologies will enable the Portfolio to manage the volume of its biometric data holdings and to leverage improvements in biometric matching, coupled with the ability to analyse large biometric databases. Advances in automation will free up resources, allowing the Portfolio to focus on prioritised and risk-based work.

This evolution of identity and biometric technologies presents transformational opportunities for the Portfolio to connect all phases of our border management, security, regulatory and law enforcement operations, enhancing our ability to advance Australia's interests and prosperity. These same opportunities also introduce new legal, policy and operational challenges, including the need to redesign legacy, biographically-driven processes and enhancing the biometric and forensic skills of our workforce. Importantly we must fulfil our legislated requirements while balancing community expectations for expedient, digitised services within a security and privacy regime, to ensure we appropriately manage and protect personal information.

It is critical that, as we continue to evolve from traditional, in-person and paper-based services to an increasingly complex and connected digital environment, we build and maintain public trust and confidence in our ability to deliver reliable and accessible services, as well as protect and manage personal information and sensitive biometric data.

Strategy purpose

The Strategy articulates a collaborative biometrics vision for the Portfolio and sets out:

- principles for the use of biometrics, information sharing, privacy protections and capability development
- direction for a governance framework and shared standards to guide future interoperability, alignment and sustainment of biometrics capabilities
- guidance for the Portfolio to achieve its biometric capability goals with a view to measuring strategic outcomes.

The Strategy addresses the risks and opportunities biometrics present to the Portfolio and through agreed goals, articulates the direction for biometrics management, within the context of the *National Identity Security Strategy 2012*. It recognises each agency's responsibilities for biometrics capabilities and harnesses opportunities to align and improve connectivity, working together, despite our use of different technologies. This approach will ensure we are well positioned to transition to new, automated and streamlined ways of working enabled by biometrics.

Through a dedicated Privacy and Ethics Framework (at Appendix A) the Strategy commits the Portfolio to data protection through clear and comprehensive policy regarding appropriate biometric collection, storage, use, and disclosure, strong governance, rigorous assurance and reporting processes that include regular internal and external oversight of systems and procedures associated with biometrics.

The Strategy supports the enhancement and sustainment of our biometric capabilities and sets direction for shared standards to guide future interoperability and capability alignment domestically and internationally, including aligning with internationally accepted standards where appropriate.

Developed in consultation with key partner agencies, this Strategy builds on the government's commitment to interconnectedness across government, delivering security and prosperity through integrated, seamless service delivery and joined-up capabilities.[2]

2. The Hon Scott Morrison MP, Prime Minister, speech to the Institute of Public Administration on 19 August 2019, Parliament House, referred to "the need for an APS that's more joined-up internally and flexible in responding to challenges and opportunities… Government needs to connect instantaneously and seamlessly" https://www.pm.gov.au/media/speech-institute-public-administration, accessed on 03/09/2019.

HOW AND WHY WE USE BIOMETRICS

What are biometrics?

A biometric characteristic is a biological or behavioural characteristic of an individual from which distinguishing, repeatable biometric features can be extracted for the purpose of biometric recognition.[3] Biometric data includes facial or voice features, signatures, fingerprints, retina patterns and gait.[4] These characteristics are subject to relatively little change compared to other types of personal information, and can be digitised for automated and secure storage, searching and retrieval.

3. International Organization for Standardization (ISO) definition (ISO/IEC 2382-37). Information technology—Vocabulary—Part 37: Biometrics, accessed on 05/08/2019; https://www.biometricsinstitute.org/what-is-biometrics/.
4. Ibid

Biometrics use a variety of technologies as a tool for recognising individuals based on measurement and analysis of their biological and behavioural characteristics.

The Portfolio's use of biometric data includes face recognition, fingerprint identification and DNA matching.

Why we use biometrics in the Home Affairs Portfolio

Biometric data links information at the core of the Portfolio's intelligence, law enforcement and operational capabilities. It enables effective and efficient verification and identification of individuals in many scenarios across the Portfolio including immigration, border protection, criminal investigations, disaster victim identification, intelligence and the provision of government services.

These capabilities are aimed at automatically verifying the biometric claim of an individual against a previously enrolled reference or to automatically identify biometric characteristics collected in a set of one or more biometric references. In cases where human assessment of automated biometric comparison decisions are required, Portfolio agencies rely on staff who are specially trained to undertake such assessments.

The Portfolio relies on trusted biometric data that complies with international standards to enable future interoperability.[5] Face and fingerprint recognition, and DNA matching are the Portfolio's core biometric modalities. However the use of other biometric modalities will enhance scalability and operational effectiveness of the Portfolio's biometric capabilities.

Use of multiple modalities to verify identity will become increasingly common in the future, both to mitigate advances in criminal capabilities seeking to misuse identities, as well as to minimise errors in the recognition process.

Figure 2: Use of biometrics across the Portfolio

- for trusted, protected and assured identities
- for streamlined government service delivery
- to support seamless high volume travel
- for victim identification and emergency management response
- for informed intelligence and risk identification
- for criminal investigation, including disruption, prevention and prosecution.

5. Trusted biometrics are biometrics collected electronically, using encrypted chip technology, from a machine readable biometric passport, or travel document, issued by an accepted authority and captured to an agreed standard in a reputable process.

Our Portfolio biometrics roles and capabilities

The Portfolio has responsibility for significant biometrics capabilities, including national face matching services, law enforcement systems, international data sharing arrangements and border gate technology. We use our combined biometrics capabilities as an enabler for identification, digital service delivery, data fidelity, automation, and boosting law enforcement, intelligence analysis and security operations.[6]

The Portfolio plays a key role in provisioning multi-user, national biometrics matching platforms and driving standards of biometrics collection to support the transition from traditional paper-based and over-the-counter forms of identity proofing to the Australian Government's new digital-identity ecosystem.[7]

We also have a unique role as a commencement-of-identity issuing and verification authority for establishing the trusted and secure identity of foreign nationals, which is then relied upon by Government agencies at the Commonwealth, state and territory level, by the judicial system, across international borders and in the private sector.

This has now become increasingly important as the Portfolio looks to enduring capabilities to enable a technology-led response to COVID-19, future pandemics and other biosecurity threats into Australia. A confirmed identity that is biometrically anchored at the first interaction with the client, and verified against that biometric anchor at subsequent interactions, will provide the foundation that links a traveller's information across the border continuum, including visa, health, travel history, intelligence and border processing.

Offshore collection of biometrics from all visa applicants is the best mechanism to achieve this, increasing access to biometrics from overseas visitors. Together with technology advances in smart device collection and data share arrangements with our partners, the move to 100 per cent biometric collection will enhance our ability to protect and advance Australia's prosperity and build national resilience.

6. Data fidelity is the degree or exactness with which something is copied or reproduced. It refers to the accuracy, reliability, consistency and security of the information.
7. The digital identity ecosystem is a digital identity program that will allow more government services to be available to people and businesses online at any time. Digital Transformation Agency. Digital identity ecosystem. [online] Available at: https://www.dta.gov.au/our-projects/digital-identity/digital-identity-ecosystem

Figure 3: Portfolio agency biometric roles

Australian Border Force

- Uses biometric technology to establish, resolve or assure the identity of citizens and non-citizens.
- Support seamless service delivery and make targeted interventions to prevent harm to the nation or our community.

Australian Criminal Intelligence Commission

- Hosts national systems for biometrics services including finger and palm print matching and DNA matching and information databases for forensic purposes to identify missing persons and disaster victims.

Australian Federal Police

- Identification and verification in support of criminal investigations, disaster victim identification and missing persons.
- Proactively supports all phases of law enforcement operations to contribute to intelligence led policing and achieve an enhanced intelligence picture.

Australian Security Intelligence Organisation

- Uses biometric data for identity verification and identification to enhance national security.
- Engages with Portfolio partners to support and use biometric capabilities.

Australian Transaction Reports and Analysis Centre

- Collects reports from regulated business to develop actionable financial intelligence for combating money laundering, terrorism financing and other serious crimes.
- Disseminates the limited biometric information collected as part of these reports to Portfolio partners.

Department of Home Affairs

- Anchors the identity of non-citizens for trusted commencement of identity in the Australian community.
- Uses biometrics to facilitate visa and citizenship services and travel to Australia.
- Identifies imposters and threats to the integrity of the migration program through international data sharing and intelligence analysis.

The Portfolio's advanced use of biometric data includes world-leading biometric and forensic applications in many areas of national security and law enforcement. Within tight fiscal constraints and limited resources, particularly in remote and regional areas, the use of biometric technologies supports efficient identification and verification requirements and provides opportunities for centralised specialist support.

The Portfolio's approach centres on tailoring biometric data to be accessible to Portfolio agencies to maximise capability outcomes, prevent duplication of effort and to ensure that data is secure and trusted for identity purposes.

This functionality enables each agency to best utilise biometric information for multiple purposes through real-time interoperability. Coordinated capability development also supports a national view of criminal intelligence and information.

Detailed information about individual Portfolio agency roles is at Appendix B. A list of biometric modalities and their uses in the Portfolio is at Appendix C.

OUR VISION

Our vision for biometrics is closely linked to the Portfolio's mission as set out in the *Blueprint for Home Affairs*.

Working together for the ethical, lawful, secure and innovative use of biometrics for the public good

OUR APPROACH

This Strategy is underpinned by six core principles, based on the Portfolio's vision, and shaped by Australian Public Service values of commitment to professional, objective, innovative and efficient service that is accountable, respectful and ethical.[8] These core principles guide the implementation of our goals and are grouped under six themes: biometric data, community, our people, governance, systems and partnerships.[9]

Our approach is strengthened by a strong privacy and ethics framework, which has been developed as a standalone document to provide clear direction for our work.

8. Australian Public Service (APS) Values are set out in Section 10 of the *Public Service Act 1999*.
9. These themes are also referred to as fundamental inputs to capability i.e. key elements that underpin the development of capability.

Biometric data

PRINCIPLE 1:
Biometric data streamlines identification and verification

The use of biometric data collected through accessible and reliable technology enables us to anchor and resolve a unique identity and link information at the core of our identity, intelligence, migration, border, regulatory and law enforcement operational capabilities. The move to 100 per cent collection of biometrics will commence trusted identities within a national identity system of reliance, enabling seamless digital government interactions and simplified access to services.

Biometric data raises our confidence level in relation to a person's identity and can reduce the need for repeated and unnecessary collection of personal and private documentation.[10]

Biometric data informs intelligence analysis and risk management and enhances intelligence functions between our domestic and international partners to protect the integrity of our programs.

We are expanding the use of trusted biometric data to leverage transformational opportunities. This includes moving from transaction-based processing to a single identity model, where biographic information is anchored to biometric data to significantly improve the accuracy of identification and verification processes. At the same time, we are reducing the complexity of identity proofing and the number of credentials required.

As an evolving discipline, we recognise the potential vulnerabilities and limitations of biometric systems. We lead government best practice, applying a low tolerance threshold for potential errors and inaccuracies that reflects the sensitive nature of biometric information, and have control measures in place to mitigate the risks.

Goal 1.1: Anchor biographical information to quality biometrics to commence trusted and reliable identities

We will achieve this by:

- Collecting 100 per cent of biometrics for every person who crosses our border, captured through a reputable process or ePassport
- Conforming with capture standards and embedding government best practice
- Enhancing multimodal biometrics to improve identification and increase national security

10. Within law enforcement, repeated collection of a person's biometrics is a common and necessary practice to improve data and prove identity for criminal record purposes.

Goal 1.2: Improve the data fidelity and accessibility of information

We will achieve this by:

- Uplifting the quality of biometric data to improve matching accuracy and resolving records to improve efficiency
- Increasing the automation of record resolution using biometric data
- Embedding processes to improve algorithmic performance and accuracy rates

Goal 1.3: Improve risk identification by leveraging domestic and international data sharing to provide pathways for streamlining and automation

We will achieve this by:

- Collecting fingerprints for migration and border operation purposes based on risk, or as a result of being in police custody, charged or a court order
- Using biometric data and technology to improve threat detection and the accuracy of alerts

Goal 1.4: Simplify service delivery

We will achieve this by:

- Using advances in smart devices and other technologies to increase the collection of biometrics domestically, as well as outside Australia
- Increasing identity verification using biometrics in place of traditional identity-proofing methods and collection of unnecessary or unreliable documents

Community

PRINCIPLE 2: Trusted custodians of biometric data

As custodians of significant biometric data holdings and owners of biometric capabilities, we are accountable for the balanced and appropriate use of biometric data.

Whether for law enforcement, national security or victim identification, our use of biometric data is prescribed by law and consistent with our obligations under the Privacy Act, Australian Privacy Principles (APP) and the *Archives Act 1983*, as applicable.[11]

We understand that the biometric data we hold is important to individuals and a data breach or unintended use could have an adverse impact on individuals' lives. To this end, we prioritise the safeguarding of personal information to protect these valuable biometric assets.

11. Some Portfolio agencies, such as ASIO and ACIC, are not APP entities which means they are not subject to provisions in the *Privacy Act 1988*. However, such agencies are governed by a range of legal and oversight mechanisms to ensure they act with due and proportionate consideration to privacy in carrying out their mandated functions.

Goal 2.1: Balance community safety, law enforcement, national security and efficient service delivery with an individual's right to privacy and control of their biometric information

We will achieve this by:

- Including privacy impact assessments in the design and development of biometric systems and proposed uses of biometric data[12]
- Collaborating across government and with industry to conform to international standards and developing government best practice for sharing biometric data

Goal 2.2: Minimise intrusions on privacy

We will achieve this by:

- Collecting a reasonable amount of biometric information necessary to achieve the purpose for which it was collected, and only using it as guided by our legislative and privacy obligations
- Adhering to obligations under the Australian Privacy Principles regarding notice to individuals when collecting biometric data

Goal 2.3: Build and foster public trust in the Portfolio as lawful custodians and users of biometric data

We will achieve this by:

- Communicating to the public to build awareness of how their data is used and for what benefit, and how individuals can access and correct their biometric information, in accordance with the Australian Privacy Principles
- Designing robust and transparent governance frameworks to ensure confidence in the security, protection and responsible use and storage of personal identifiable information
- Strengthening and promoting independent oversight arrangements for the Portfolio's biometric capabilities and practices

12. APP 1 requires APP entities to take reasonable steps to implement practices, procedures and systems that will ensure compliance with the APPs and enable them to deal with enquiries or complaints about privacy compliance. Reasonable steps include undertaking privacy impact assessments, a systematic assessment of proposal or change that identifies the impact that the change might have on the privacy of individuals, and sets out recommendations for managing, minimising or eliminating that impact.

Our people

PRINCIPLE 3:
Shared biometric expertise and services across the Portfolio

Our people are our most valued asset. We put in place strategies to recruit, train and retain people with the right skills and aptitude to ensure continuous high quality capabilities and service delivery. We invest in training and continuous professional development for all staff, from frontline officers to identity resolution and forensic specialists, to meet the increasing demands on immigration, border protection, intelligence and law enforcement.

Sharing our respective expertise and services helps us to leverage our collective strengths in support of Government priorities. Our specialist biometric and forensic capabilities enable the verification of identity and identification of unknown or unresolved biometrics, for law enforcement, security, regulatory, immigration and border-related functions. We provide shared services across the Portfolio to support national and international identity verification requirements, enable sound decision making and ensure just outcomes.

We are harnessing identity and biometric expertise to build capability through multi-disciplinary teams. Supported by technologies that automate low value work, our enhanced workforce will focus on integrity and prioritised risk.

We are investing in the development of qualified specialists to analyse biometric data to help us inform standards and algorithmic thresholds to identify threats, optimise our operations, reduce duplication and complement our workforce capacity.

Goal 3.1: Work collaboratively to build enhanced biometric capability

We will achieve this by:

- Building the identity, biometric and forensic skills and capabilities of people through multi-disciplinary teams across the Portfolio, leveraging common technical and specialised skillsets
- Leveraging respective Portfolio biometric training resources and consolidating to achieve capability alignment, greater interoperability, and efficiencies where appropriate
- Establishing a community of practice for Portfolio biometrics experts to drive strategic capabilities and initiatives
- Building on partnerships with academic institutions to co-design and deliver tailored qualifications in forensic biometrics and biometric technologies
- Creating opportunities for cross-skilling across government and with international partners

Goal 3.2: Build a centre of biometric expertise

We will achieve this by:

- Strengthening national biometrics capabilities to provide identity and biometric services, including 24/7 networks, for law enforcement, immigration and citizenship services and border operations
- Establishing identity resolution capability and strengthening referral mechanisms for the consistent treatment of risk, fraud and crime

Governance

PRINCIPLE 4: Robust and transparent biometrics management through strong legislative, policy and procedural frameworks

While each agency is governed by different legislative and operational requirements, our management of biometric data is consistent across the Portfolio, underpinned by clear policies and procedures that guide lawful and ethical collection, use, storage, disclosure, retention and data sharing.

As new biometric technology is deployed, it is important to determine standards and processes for secure, trusted and accessible data for identity purposes across the Portfolio, and to identify and prevent duplication of effort.

We have strong program governance and reporting mechanisms that include regular internal and external oversight of all biometric related systems and operations.

As biometric capability owners we are responsible for the investment and sustainment of all fundamental elements: our people, processes, data and technology.

Goal 4.1: Ensure data is collected, used and shared for a lawful and specified purpose

We will achieve this by:

- Establishing a data security framework that provides security settings for data held by critical infrastructure owners and operators
- Increasing awareness of legal provisions relating to data sharing to ensure interoperability meets statutory requirements and developing ethical policies where legislation doesn't provide clear direction

- Collaborating across Government and with industry to establish government best practice, adhering where possible to international standards for the collection, use, storage, disclosure and disposal of all existing, emerging and future biometric data[13]
- Reviewing compliance with the Australian Privacy Principles in processes relating to consent and notification of collection, use, storage, disclosure and sharing of biometric data
- Designing and implementing robust, transparent policy and procedures for the lawful management of biometric data

Goal 4.2: Secure and protect biometric data holdings and technologies

We will achieve this by:

- Reviewing controls to appropriately safeguard biometric data holdings and minimise the risk of unauthorised use, unintentional disclosure or destruction, and cyber-security breaches
- Ensuring mandatory minimum training requirements, including those relating to privacy and data security are completed before accessing technology
- Operating within Portfolio capability frameworks that support the sustainment and development of capability including roadmaps and end of life system management

Systems

PRINCIPLE 5: Connected systems built on common architectural principles

The public and Government expect interoperability between agencies and across government. Our system enhancement and innovation is driven by the need to communicate and work seamlessly together and share data, despite our reliance on and use of different technologies.

We acknowledge the importance of collaborative system design, aligning and consolidating biometric systems to maximise efficiencies and reduce duplication, to enhance operational effectiveness. Usable solutions, engineered with end-user requirements in mind, will result in higher effectiveness and system performance.

13. Some Portfolio agencies, such as ASIO and ACIC, are not APP entities which means they are not subject to provisions in the *Privacy Act 1988.*

We make sensible procurement decisions, taking into consideration existing capabilities, to invest in biometric technologies that are adaptable across a range of Portfolio responsibilities. We align our new systems with international standards to prevent vendor-specific technology, lack of interoperability and increased resourcing/costing imposts.

We advocate for investment to deploy accessible, functional and usable technologies at sea and in other remote and regional areas where digital connectivity presents challenges. We understand 'real time' accessibility supports operational requirements, workforce agility and reduces operational risks.

We strive for multimodal biometrics capabilities to enhance scalability and operational effectiveness. However, facial images, fingerprint biometrics and DNA will remain as the Portfolio's core modalities.

Our biometric systems will be a costed and managed service, enabling businesses with biometrics dependencies to subscribe to our capabilities and services.

Goal 5.1: Increase interoperability across Portfolio agencies utilising biometric technology

We will achieve this by:

- Aligning architectural principles and standards in accordance with information protocols to encourage consistency and flexible adaptation

Goal 5.2: Improve the management of high volume data to support digital service delivery and travel facilitation

We will achieve this by:

- Modifying legacy systems to support the electronic collection of biometric passport information and facial images
- Maximising biometric matching and automated identity resolution
- Investing in machine learning and artificial intelligence technologies, harnessing innovation and adapting systems to address new challenges

Goal 5.3: Support considered and sensible procurement of usable technologies to innovate and address new challenges

We will achieve this by:

- Aligning with international standards to prevent vendor specific technology, improve interoperability and reduce resourcing impacts
- Reducing duplication by adapting or consolidating existing systems where they can serve several purposes or provide similar services
- Attracting investment to support the sustainment of our people, processes, data and technology in order to achieve full utility of our biometric capabilities

Partnerships

PRINCIPLE 6:
Enduring partnerships and strengthening capabilities

Strategic partnerships are a priority in an increasingly connected world. We are leaders in the development and delivery of biometrics capabilities and share these with our trusted partners. We work across government, leveraging opportunities to collaborate, innovate and streamline. We continue our capacity building efforts by encouraging the adoption of biometric capabilities in our international regional partners' strategies, policies, intelligence and operational systems.

It is important that we progress a broader data exchange agenda with a wide range of trusted national and international partners to improve threat detection, risk identification and countering transnational serious and organised crime outside Australia.[14]

To facilitate the passage of legitimate travellers to Australia and partner countries, the Portfolio will extend international biometric-sharing arrangements and border data exchange schemes. Streamlined border service delivery depends on effective management of increasing throughput. To support this, we will collaborate and co-design investment with our industry partners and other governments.

We contribute to international biometric standards design and the promotion of best practice to influence and shape world-leading biometrics innovation.

Goal 6.1: Promote best practice to influence and shape world-leading biometrics innovation

We will achieve this by:

- Expanding partnerships for biometric collection service delivery in and outside Australia
- Analysing identity and biometric-related fraud and crime to inform trust levels in passport issuing authorities
- Increasing biometric data sharing with partners, such as state and territory government agencies, national, regional and international law enforcement partners, Migration 5, Border 5 and trusted international migration partners
- Engaging and collaborating with industry to prepare for co-design and co-investment on biometric-facilitated travel
- Boosting co-design with industry and academic institutions to remain at the forefront of innovation and to better understand the public impact of biometric technologies

14. Any data sharing initiatives will recognise Portfolio agencies have specific legal and policy frameworks that govern the sharing of sensitive personal data.

- Elevating participation through direct engagement with international forums to lead and contribute to the development of international biometric standards design and shape world-leading biometrics innovation
- Continuing to engage with advisory groups that shape and influence standards in training and methodologies

Goal 6.2: Expand biometric data sharing technologies and arrangements to improve risk and threat identification

We will achieve this by:

- Collecting fingerprints for migration purposes based on risk to leverage Migration and Border 5 and Five Eyes partnerships
- Developing government and industry interoperability options to support strengthened information sharing to prevent threats emerging and detect persons of concern
- Supporting capacity building through the adoption of biometrics capabilities in our regional partners' strategies, policies, intelligence and operational systems
- Bolstering regional and international biometric data-sharing capabilities

WHAT SUCCESS LOOKS LIKE

The future state of the Portfolio's use of biometrics is driven by the growth of biometric technology and the demand for streamlined service delivery. In order to realise the opportunities this presents, we will continue to develop our biometrics and forensic expertise and ensure we have the required capabilities to realise our goals. This will be enabled by harnessing technology and empowering our staff to embrace sustained and aligned agency activity to support the breadth of the Portfolio's functions. These efforts will ensure the Portfolio is positioned to respond to new challenges and to contribute to a secure, prosperous and united future. The following diagram illustrates the future state which will be enabled through this Strategy.

THEME	FUTURE STATE
Biometric data	We capture biometric data with a high fidelity to anchor and resolve a unique identity
	The use of biometric data results in safer communities and just outcomes
Community	The Australian community trusts the Portfolio to use and manage biometric data
	We collect the appropriate amount of biometric data required to enable decision-making
Our people	Multi-disciplinary teams manage biometric data in an operational context
	Portfolio staff build biometric skills and expertise through a community of practice and shared training resources
Governance	Our governance framework protects our biometric data holdings
	We have strong policy and procedural frameworks and clear legislative parameters
Systems	We use interoperable biometric systems to support a range of functions
	We deliver streamlined services enabled by biometric recognition
Partnerships	Our biometric innovation shapes international best practice
	We increase biometric data sharing and matching with trusted partners

EVALUATING THE STRATEGY

The Strategy's goals, identified in *Our Approach*, provide the foundation for defining measurable results that the Portfolio seeks to achieve. However, we recognise that the pace of technological advancement may result in the need for us to revise and adapt the Strategy's future state over the course of its five-year lifespan.

To give life to the Strategy, an inter-agency Working Group has been formed to drive an implementation plan and deliver work packages related to fulfilling the goals outlined in the Strategy. The Working Group will be overseen by a high level Portfolio Biometrics Steering Group, which will provide strategic guidance and ensure alignment of efforts across the Portfolio.

The Steering Group will undertake annual reviews of the Strategy, commencing 12 months after its implementation, in order to evaluate measurable results and determine whether its goals require reconsideration. To promote the Strategy's shared ownership, the role of the Steering Group chairperson will be rotated across the Portfolio every 12 months, with the chairperson's agency providing secretariat support for the duration of their tenure.

APPENDICES

APPENDIX A: Home Affairs Portfolio privacy and ethics framework for the management of biometrics

This framework sets out principles which guide the work undertaken across the Portfolio to ensure privacy and ethics are at the forefront of the Portfolio's work in relation to biometrics. The principles outlined in this framework have been incorporated throughout this Strategy.

Privacy protection

The Portfolio will ensure privacy protection in the following ways:

- Protecting privacy through the use of biometrics to prove identity, rather than repeated collection of personal and private documentation
- Protecting biometric data from theft, misuse, interference and loss, and from unauthorised access, modification or disclosure
- Collecting biometric data only as reasonably necessary
- Considering the privacy implications of the collection, use, storage and retention of an individual's biometric information before, during and after the operation of services
- Undertaking privacy impact assessments when developing new ways to collect, use, store and disclose biometrics[15]
- Monitoring and enhancing privacy and security measures to protect biometric data (such as through audits, access security controls, staff training, and procedures for responding to or reporting privacy breaches)

Ethical and lawful

The Portfolio will promote the ethical and lawful use of biometric data in the following ways:

- Collecting, using, storing, retaining and disclosing biometric data only for lawful and specified purposes
- Using robust evidence to inform procedures on the use of biometric services
- Embedding processes to ensure data accuracy, error detection and repair

15. APP 1 requires APP entities to take reasonable steps to implement practices, procedures and systems that will ensure compliance with the APPs and enable them to deal with enquiries or complaints about privacy compliance. Reasonable steps include undertaking privacy impact assessments: a systematic assessment of proposal or change that identifies the impact that the change might have on the privacy of individuals, and sets out recommendations for managing, minimising or eliminating that impact.

- Balancing community safety and national prosperity with an individual's right to privacy
- Adhering to obligations under the Australian Privacy Principles regarding notice to individuals when collecting biometric data[16]
- Taking particular account of the rights of children and vulnerable people
- Strictly adhering to legal frameworks for disclosing and sharing of biometric data between agencies, and with partners across borders and jurisdictions

Transparent and accountable

The Portfolio will be transparent and accountable in its use of biometrics in the following ways:

- Operating in line with legal and governance frameworks (including comprehensive governance to guide implementation of the Strategy)
- Communicating biometric capabilities and limitations to the public to provide clarity and promote understanding about the use of biometric data
- Strengthening and promoting independent oversight of development and use of biometric capabilities

Explanatory note

Our use of biometric data is prescribed by law, through the relevant Acts that regulate our work. How we collect, use, disclose and store personal information is governed by the Privacy Act, and includes the Australian Privacy Principles (APPs) and the intersecting provisions of the *Archives Act 1983* relating to the provision and disposal of personal information contained in a Commonwealth record. Some Portfolio agencies, such as ASIO and the Australian Criminal Intelligence Commission, are not APP entities which means they are not subject to provisions in the Privacy Act. All interactions that Portfolio staff have with biometric data must be consistent with the APS Code of Conduct, set out in the *Public Service Act 1999*, and equivalent Codes of Conduct for statutory agencies. This includes behaving honestly and with integrity, acting with care and diligence and upholding the APS Values.

Collecting and using biometric data for specific purposes

In accordance with APP 6, the Portfolio will use or disclose biometric data for the primary purpose (being the purpose for which the information was collected). Noting the breadth of the Portfolio's functions, APP entities may also rely on APP 6.2 or 6.3 to use or disclose biometric data for a secondary purpose, such as where the use or disclosure is required or authorised by law or where the use or disclosure is reasonably necessary for an enforcement related activity of an enforcement body.

16. Some Portfolio agencies, such as ASIO and ACIC, are not APP entities which means they are not subject to provisions in the *Privacy Act 1988.*

For example, the primary purpose of collecting a passport image is to create a passport. However, the Face Identification Service (FIS) will enable the use of passport images for a secondary purpose such as where to do so is reasonably necessary for an enforcement related activity of an enforcement body.

Providing notice and obtaining consent

The Portfolio has obligations under the Privacy Act regarding notice and consent when collecting information. APP 3 requires APP entities to obtain consent when collecting biometric data unless an exception applies. Under APP 3.4, APP entities may collect biometric data without an individual's consent where it is reasonably necessary for an enforcement related activity or where the collection is required or authorised by law.

APP 5 places an obligation on the Portfolio to take reasonable steps to notify an individual or otherwise ensure that they are aware of certain matters, at or before the time of collecting personal information. In some circumstances, it will not be reasonable for an APP entity to provide notice to individuals as noted in the APP Guidelines at 5.7. For example, this may occur where notification could pose a threat to public health or safety, or jeopardise the purpose of collection where there is a clear public interest in the purpose of collection. Where the Portfolio considers that it is reasonable not to take steps to provide a notice or ensure awareness of the matters in APP 5 the Portfolio is responsible for justifying not taking any steps.

APPENDIX B:
Biometrics roles by agency

Australian Border Force

The Australian Border Force (ABF) is a law enforcement agency, responsible for offshore and onshore border control enforcement, investigations, compliance and detention operations in Australia. The ABF uses biometric technology to establish, resolve or assure the identity of citizens or foreign nationals. The verification of a person's identity is critical to the ABF's operations. This gives us the confidence to provide seamless facilitation or service delivery and to make targeted interventions to prevent harm to the nation or our community.

The ABF is strengthening its capabilities to best support intelligence, technology, practices and people to achieve business objectives and manage risks. More convenient collection and access to biometric data allows for greater automation and facilitation of travellers across Australia's borders, allowing the ABF to focus on areas of high risk and exceptions.

Australian Criminal Intelligence Commission

The Australian Criminal Intelligence Commission (ACIC) hosts national systems for biometric services including finger and palm print matching and DNA matching. The agency also hosts information databases for forensic purposes for the identification of missing persons and disaster victims.

National Automated Fingerprint Identification System

National Automated Fingerprint Identification System (NAFIS) is the only national fingerprint and palm print database and matching system and is used extensively by police agencies to help solve crime and identify individuals. NAFIS is centrally hosted by the ACIC. NAFIS has been operational nationally since 1986 for policing agencies and also contains biometrics provided by INTERPOL as well as fingerprint holdings collected by the Department of Home Affairs.

National Criminal Investigation DNA Database

The National Criminal Investigation DNA Database (NCIDD) allows Australian police to match DNA profiles across Australian jurisdictions and establish the identity of persons of interest from human biological samples. It is a centralised national DNA database with direct matching capability. The NCIDD provides Australian police and forensic scientists with an intelligence tool that crosses jurisdictional boundaries. It is an online entry web-based application designed to view potential links between DNA records both at a jurisdictional and inter-jurisdictional level.

NCIDD Integrated Forensic Analysis

The NCIDD Integrated Forensic Analysis (NCIDD-IFA) provides Australian police jurisdictions and related agencies with forensic software to enable familial searching, kinship matching and advanced direct matching across Australia's state and territory borders for law enforcement purposes.

Australian Federal Police

The Australian Federal Police's (AFP) role as the Australian Government's primary law enforcement agency is to enforce Commonwealth criminal law, contribute to combating complex, transnational, serious and organised crime impacting Australia's national security and to protect Commonwealth interests from criminal activity in Australia and overseas. The AFP also has responsibility for providing policing services to the Australian Capital Territory and Australia's territories, including Christmas Island, Cocos (Keeling) Islands, Norfolk Island and Jervis Bay.

AFP Biometrics is one of a number of forensic specialist capabilities within the Operational Science and Technology Specialist Operations Portfolio. AFP biometrics capabilities, including fingerprints, DNA and facial identification, are deployed in collaboration with other specialist capabilities to achieve operational impact. AFP Biometrics is focused on the development, collection, storage and analysis of scientific evidence for the purposes of identification in support of criminal investigations, disaster victim identification and missing person's cases, The capabilities are maintained, advanced and delivered through leadership, collaboration, learning and innovation.

Biometric capabilities have evolved to proactively support all phases of law enforcement operations through prevention, disruption, investigation and prosecution. As a result, AFP Biometrics is well-positioned to contribute to intelligence led policing to achieve an enhanced intelligence picture.

The AFP works closely with a range of law enforcement and government agencies at state, territory, Commonwealth and international levels, including in its role as Interpol's National Central Bureau (NCB) in Australia for the provision and exchange of biometrics internationally to enhance safety and provide a secure regional and global environment.

Disaster Victim Identification

Disaster Victim Identification (DVI) is a process to correctly identify deceased victims of a disaster or incident where there are multiple fatalities or where the identity of deceased victims is in dispute, before returning them to their respective families.

The AFP has a DVI capability with assigned DVI commanders for the ACT, national and international responses. The capability is coordinated through the DVI Executive Steering Committee chaired by the Chief Forensic Scientist.

Australian Security Intelligence Organisation

The Australian Intelligence Organisation (ASIO) is Australia's national security intelligence service. ASIO provides advice to the Australian Government on threats to national security. ASIO uses biometric data for identity verification and identification to enhance national security.

ASIO intends to use Portfolio biometric capability to assist in the verification of identity and identification of subjects relevant to security in a timely and accurate manner. Access to the biometric data collected and held by the Portfolio supports ASIO's investigative role across all of their mandated responsibilities.

Australian Transaction Reports and Analysis Centre

The Australian Transaction Reports and Analysis Centre (AUSTRAC) is Australia's financial intelligence unit and anti-money laundering and counter-terrorism financing regulator.

AUSTRAC regulates financial institutions and providers of gambling, remittance, digital currency and bullion services that have obligations under the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (AML/TF Act). These obligations centre on identifying and verifying customer identity, providing reports to AUSTRAC about financial transactions, and implementing systems and controls to identify, mitigate and manage money laundering and terrorism financing (ML/TF) risks.

The bulk of AUSTRAC's financial intelligence comes from the wealth of information provided in the reports submitted by regulated businesses to AUSTRAC about financial transactions, and the customers involved in these transactions. AUSTRAC analyses and disseminates the information as actionable intelligence to our partner agencies in law enforcement, criminal intelligence, national security, and revenue protection to combat and disrupt criminal activity.

As part of customer due diligence, a small number of regulated businesses will capture biometric information and proactively include this information in reports provided to AUSTRAC. This biometric information is generally limited to facial images depicted on CCTV footage or identity documents, and voice recordings. These become part of 'AUSTRAC information' for the purposes of the AML/CTF Act and are accessed and disclosed in accordance with the secrecy and access provisions of that Act.

Department of Home Affairs

Domestic and International Biometric Data Sharing

Biometrics were first used in the Department of Home Affairs (the Department) for the detention caseload and now includes the collection of facial images and fingerprints from certain visa applicants and interdicted persons at the border. Offshore collection occurs in over 50 countries and allows the Department to mitigate risk offshore, away from the Australian border. It is a critical enabler for the facilitation of streamlined travel for bona-fide visitors and the digitalisation of our visa services.

The Department currently relies on facial images and fingerprints as its primary biometrics. The choice of the biometric modality is influenced primarily by how convenient it is to collect and enrol the data, matching accuracy and the availability of data holdings for comparison and matching purposes.

While face biometric matching is automated the matching accuracy is probabilistic, resulting in a higher margin of error, compared with other modalities such as fingerprints. Matching algorithm thresholds are set to compliment manual resolution capacity. Acceptance of higher error rates can be mitigated by investing in training facial specialist resources to undertake manual identity resolution work.

Facial biometrics benefit from widely available, high-performance camera systems. The use of face recognition technology has become the preferred approach at our borders, in collaboration with aviation security partners, to deliver improved traveller facilitation across the entire passenger experience from reservation to boarding. It is also the modality of choice for future streamlined facilitation of online visa service delivery. Facial image standards continue to mature and there have been exponential improvements in face matching speed and accuracy. Face data exchange has also been widely adopted and used for identity verification throughout civil aviation.

Fingerprint biometrics provide high match performance and accuracy and enable risk identification across Australian law enforcement databases and international partners' immigration and criminal data holdings. Fingerprint matching can provide potential pathways for automation and recurrent checking, while requiring low level human resource support.

Collection and verification of biometrics also occurs at the border. The Department shares data with Migration Five (M5) partners, and on a case-by-case basis with other government agencies, including state and territory law enforcement. Biometric matching is undertaken against our own biometric data holdings and against the holdings of international partners to provide pathways for streamlined visa and citizenship decision-making. Fingerprints matched against M5 partners: the United States, United Kingdom, Canada and New Zealand can detect fraud, security and criminality concerns.

National Facial Biometric Matching Capability

In collaboration with states and territories, Home Affairs is developing a National Facial Biometric Matching Capability (NFBMC). The NFBMC provides new national Face Matching Services that can be used by a broad range of government agencies to help verify a person's identity and prevent the use of fake or stolen identities. A smaller number of security and law enforcement agencies can also use the services to identify people who are suspects, or victims, of terrorist or other criminal activity. It will also prevent the use of fake or stolen identities.

While maintaining lawful privacy safeguards, agencies in all jurisdictions will be able to use new face matching services to access passport, visa, citizenship, and drivers licence images. Importantly, the system does not provide for automated or 'real time' mass surveillance of public spaces. Nor can it use live CCTV feeds to identify a face in a crowd. However, it does support more targeted searching by using still images—taken from CCTV, for example—to quickly identify a person of interest.

Enterprise Biometrics Identification Service

The Department is deploying the Identity Management Service (IMS) and the new Enterprise Biometrics Identification Service (EBIS) to provide a centralised identity resolution, management and storage platform, replacing old biometric architecture no longer capable of supporting significant increases in biometric and biographic transaction volumes.

EBIS is a multimodal biometric verification solution supporting face and fingerprint biometrics. It is designed to manage an initial 250 million facial and fingerprint images and maintain annual growth of over 75 million from visa, citizenship and border operations.

The new system is exponentially more accurate due to its state-of-the-art biometric matching algorithms and can process over 200,000 biometric matching transactions daily. EBIS will deliver much larger-scale biometric data matching, storing, analysis, and sharing capability to improve the Department's confidence in a person's identity, and prevention of fraud.

Increased capacity through EBIS will also allow the consolidation of all facial images collected at the border into a central, searchable, data store. Under visa reform initiatives, the Department will increasingly capture ePassport facial images conveniently through smart devices and simplified visa services.

APPENDIX C:
Portfolio agency biometric capability

Biometric characteristic	Extended use/tools	Capability owner	Purpose	Description
Systems that use one or many biometric modalities	Enterprise Biometric Identification Services (EBIS)	Department of Home Affairs	Identity management, data sharing	EBIS is a biometrics storage and matching engine. EBIS services all operational areas of the Department to support national security, records management and risk identification for border and immigration purposes.
	Identity Management Service (IMS)	Department of Home Affairs	Identity matching, identity resolution, detecting identity fraud, API Gateway	A centralised identity management capability comprising a number of systems. The IMS provides increased confidence in identity matching and identity resolution.
	Secure Real Time Platform (SRTP)	Facilitated through international data sharing agreements	International data sharing	Governed by bilateral sharing agreements. The SRTP is a platform that supports identity, visa compliance and community protection related information sharing between M5 partners based on biometric matches.
	Disaster Victim Identification (DVI)	AFP	Identity verification	A process to correctly identify deceased victims of a disaster or incident where there are multiple fatalities or where the identity of deceased victims is in dispute, before returning them to their respective families.
	International Facilitation for Biometric Exchange	AFP	International data sharing	AFP Forensics is the conduit for DNA, Fingerprint and Facial imagery exchanges and mutual assistance requests with overseas law enforcement agencies and Interpol.
Face Recognition	Face Matching Services (FMS)	Coordinated and managed by Department of Home Affairs as the Framework Administrator	Biometric matching, identity matching	The FMS consists of the FVS and the FIS. The FVS enables a facial image associated with an individual to be compared against a facial image held on a specific government record associated with that same individual to confirm that individual's identity. The FIS enables a facial image to be compared against multiple images held on a database of government records to establish an individual's identity. The FMS is not a database and does not store any personal information.

Biometric characteristic	Extended use/tools	Capability owner	Purpose	Description
Face Recognition ***continued***	SmartGate	ABF	Credential verification, identity verification	Used by the ABF to perform face to passport checks using the information in a traveler's passport chip combined with facial recognition technology.
	Identity Card (ImmiCard)	Department of Home Affairs	Credential management, identity verification	Identity credential: the ImmiCard is an identity card issued by the Australian Government to undocumented non-citizens, and is used for identity verification.
	Facial Comparison	AFP and Department of Home Affairs	Identity verification, identity matching, evidentiary	Examination of facial imagery to determine if the images are of the same person, both intelligence and evidentiary products are produced using manual comparison techniques and automated comparison services.
	2D Facial Reconstruction	AFP	Identity verification	Facial biometric visualisation: Facial imagery from deceased persons is digitally reconstructed to approximate their appearance prior to death. Used to identify a deceased person, the images can then be forwarded to investigators or searched on facial recognition systems.
	Face-Fits	AFP	Identity verification, evidentiary	An input to biometric capability. Facial image construction: Witnesses are interviewed in order to generate an electronic image of a suspect/s. Used for media releases and dissemination to patrol police members.
	Facial Recognition	AFP	Identity verification	Using a standalone facial recognition system, images are searched against a database of facial images.
	Photo Boards	AFP	Identity verification, evidentiary	A board produced for identification purposes. Photographs of 11 other persons resembling the suspect are presented alongside the suspect image. The board is presented to the witness for the purpose of attempting an identification.
	Craniofacial Reconstruction	AFP	Identity verification	Recreating the face of a deceased person based on a recovered skull to assist identification. Techniques such as clay modelling and digital construction are used.
Fingerprint	National Automated Fingerprint Identification System (NAFIS)	ACIC	Identity resolution, identity matching	A 24/7 fingerprint and palm print database and matching system. Used by the Australian police agencies and the ABF to anchor and verify a person's identity from fingerprint and palm impressions.

Biometric characteristic	Extended use/tools	Capability owner	Purpose	Description
Fingerprint *continued*	Enhanced Biometrics at the Border (eBATB)	Department of Home Affairs	Identity verification, identity matching	A mobile fingerprint verification device used to access NAFIS.
	Fingerprint examination and identification	AFP	Identity verification, evidentiary	Used to establish and confirm a person at a crime scene or crime scene to crime scene. NAFIS is used to store and search.
	National Portable Biometrics Interface (NPBI)	ACIC	Identity verification, identity matching	A mobile fingerprint verification device used to access NAFIS.
Latent Fingerprints	Latent fingerprint detection	AFP	Evidentiary	Detect, visualise and record fingerprints in the field and laboratory using a variety of physical (powders), chemical and photographic techniques.
	NAFIS	ACIC	Identity resolution, identity matching	A 24/7 latent fingerprint and palm print search and matching capability, used by the Australian police agencies to identify unknown finger and palm prints from crime scenes.
DNA (Deoxyribo-nucleic acid)	National Criminal Intelligence DNA Database (NCIDD)	ACIC	Identity verification	A 24/7 database service used by all Australian police agencies to establish the identity of persons of interests from human biological samples.
	NCIDD - Integrated Forensic Analysis (NCIDD - IFA)	ACIC	Identity verification, identity matching	An enhancement of the NCIDD, including kinship matching, familial searching and advanced direct matching.
	DNA Analysis and Interpretation	AFP	Extract DNA profiles, establish identity, NCIDD store/search	DNA profiles are extracted from samples collected from the field and laboratory. The profiles are uploaded and searched on NCIDD to establish person-to-crime scene links and person-to-person links.
	National Missing Person and Victim System (NMPVS)	ACIC	Identity verification, identity matching	Used to identify victims of major accidents and disasters, long-term missing persons and unidentified human remains.
	Y STR Amplification and Analysis	AFP	Identify relations, identify lineage	Male-specific DNA analysis. For determining DNA mixtures, and resolution of paternal lineage differentiation and discrimination of closely-related males.
	Massive Parallel Sequencing (MPS)	AFP	Intelligence	Uses the information coded within DNA to predict physical characteristics of an individual in a sample collected from a crime scene or exhibit. Currently the characteristics hair and eye colour and biographical ancestry are in the validation process for operational use.

APPENDIX D: Strategic alignment

This Strategy was developed with consideration of the Blueprint for Home Affairs, other key government strategies and national frameworks, and with consideration of alignment with key Portfolio partners.

Key strategies, policies and frameworks relating to biometrics

Key national strategies, policies and frameworks related to biometrics include (but are not limited to) the following:

National identity frameworks

- *National Identity Proofing Guidelines* (2016)
- *National Identity Security Strategy* (2012)
- *An agreement to a National Identity Security Strategy* (2007)
- *National Identity Security Strategy: A National Biometric Interoperability Framework for Government in Australia* (2012)
- *Intergovernmental Agreement on Identity Matching Services 2017* (COAG)

National access policies

- Face Verification Service (FVS) Access Policy: National Facial Biometric Matching Capability v3.4 2018
- Face Identification Service (FIS) Access Policy: National Facial Biometric Matching Capability v2.4 2018

Key Partnerships

Our key partnerships with other Commonwealth, state and territory governments, industry and academia, are a priority for enhancing the Portfolio's biometric program.

We will maintain alignment with our key partners by working together to promote the responsible and ethical use of biometric data, connecting with global experts in the biometrics industry, and through participating in thought-leadership forums to stay connected, including the Biometrics Institute, and the National Institute of Forensic Sciences.

APPENDIX E: Glossary

Term	Definition
Acquire identity information	Activities that collect personal information including biographic, biometric and supporting evidence Acquiring identity information includes: • Collecting and enrolling a facial image • Collecting and enrolling fingerprints • Entering biographic information into our systems • Receiving notification of a change, such as a death, name change • Receiving information from a partner agency To successfully complete a biometric acquisition process[17]
Algorithmic performance	The ability for the biometric matching algorithm to correctly identify a match or no match of one biometric image against another biometric image or a set of biometric images within an acceptable response timeframe based on defined business requirements
Artificial Intelligence (AI)	Branch of computer science devoted to developing data processing systems that perform functions normally associated with human intelligence, such as reasoning, learning, and self-improvement[18]
Assure identity	Activities that establish the level of confidence the Department has in the genuineness of a claimed identity
Australian Privacy Principles (APP)	Provides principle-based law which set out the standards, rights and obligations in relation to: • Collection, disclosure and use of personal information • Governance and accountability • Integrity and correction of personal information • Access to personal information
Authentication	The act of proving or showing to be of undisputed origin or veracity[19]
Biographic information (Biographics)	Personal information which provides the basic elements of data about a person Biographics include: • Name • Date of birth • Sex • Gender • Nationality • Country of birth

17. ISO/IEC JTC 1/SC 37/WG 1 'Harmonized Biometric Vocabulary'
18. ISO/IEC 2382:2015 'Information Technology – Vocabulary' Note 1 to entry: artificial intelligence; AI: term, abbreviation and definition standardized by ISO/IEC [ISO/IEC 2382-1:1993].
19. ISO/IEC JTC 1/SC 37/WG 1 'Harmonized Biometric Vocabulary'.

Term	Definition
Biometric anchoring	Activity of collecting trusted biometric information and associating this with an identity record
Biometric/s	A biometric characteristic/biometric (deprecated) is a biological or behavioural characteristic of an individual from which distinguishing, repeatable biometric features can be extracted for the purpose of biometric recognition[20] Biometric data includes facial or voice recognition, signatures, fingerprints, retina patterns and gait
Biometric matching	Process of matching and comparing one set of biometric identifiers to a set of biometric records
Biometric modality/modes	Combination of the following constituents: • Biometric characteristic type • Sensor type • Processing method[21]
Biometric passport (ePassport/digital passport)	A combined paper and electronic passport that contains biometric information embedded in a chip A biometric passport contains a trusted biometric
Biometric verification	Process of confirming a biometric claim through biometric comparison[22] One-to-one biometric matching undertaken to ensure that the information provided is true or accurate when compared to source data
Border 5 (B5)	The B5 is a strategic partnership within the Five Eyes alliance, led by the heads of customs and border protection agencies from Australia, Canada, New Zealand, the United Kingdom and the United States The B5 enables cooperation, sharing and exchange of biometrics and other information to assist with joint efforts in the enforcement of customs, immigration and other border controls to maintain the security or their respective societies
Commencement of identity (COI)	Commencement refers to the first registration of a person's identity information by an Australian government agency Identity information includes: • Visa records • Australian birth certificates • Australian citizenship certificates • ImmiCards These documents are primary credentials used as the basis for verification of identity and subsequent enrolment for any high-value government or non-government service For individuals born in Australia, their birth registration with an Australian state or territory Registry of Births, Deaths and Marriages is their COI record For people born outside Australia, their COI record is their electronic visa record held with the Department of Home Affairs

20. ISO/IEC JTC 1/SC 37/WG 1 Harmonized Biometric Vocabulary
21. ibid
22. ISO/IEC 2382-37:2017-02 "Information Technology – Vocabulary – Part 37: Biometrics"

Term	Definition
Community of Practice	Networks or forums for professionals to share their practice experiences, develop and discuss areas of interests and build a sense of community
Data sharing	The process where information is shared for an agreed purpose with trusted domestic and international partners in adherence with privacy and legal obligations
Fundamental inputs to capability	Key elements that underpin the development of capability
Identity	A combination of characteristics or attributes that allow a person to be uniquely distinguished from others within a specific context
Interoperability	Computer systems or software able to connect with each other for the exchange of data and programs[23]
Manage/maintain identity information	Activities that manage an individual's identity information to maintain accuracy and accessibility include: • Updating or changing identity records • Sharing data • Storing data
Matching algorithm	Rules and procedures for determining the similarities and differences between data-sets
Migration 5 (M5)	An arrangement between five member countries, Australia, Canada, the United States, the United Kingdom and New Zealand The arrangement allows for, among other activities, the exchange of fingerprint records for matching against the immigration data holdings (of non-citizens) of each member country and the exchange of certain biographical data in the event of a match
Multimodal	At least two out of three constituents (biometric characteristic type, sensor type or processing method) of a biometric modality in a single biometric system[24]
Personal information	*The Privacy Act 1988* defines personal information as: '…information or an opinion about an identified individual, or an individual who is reasonably identifiable: a) whether the information or opinion is true or not; and b) whether the information or opinion is recorded in a material form or not.'[25]
Primary biometrics	A biometric identifier that provides the highest level of identity assurance
Resolve identity record	Activities that establish a unique and consolidated view of client information Resolving an identity record includes: • Matching biometric and biographic data • Identifying duplicate or unique records • Splitting and merging client records • Differentiating between individuals
Sensitive biometric data	Information that, as determined by a competent authority, must be protected because its disclosure, modification, destruction, or loss will cause perceivable damage to someone or something[26]

23. https://www.macquariedictionary.com.au accessed 23/08/2019
24. ISO/IEC 2382-37:2017
25. As set out in Section 6 of the *Privacy Act 1988*
26. ISO/IEC 2382:2015 'Information Technology – Vocabulary'

Term	Definition
Sensitive information	The *Privacy Act 1988* defines sensitive information as: (a) 'information or an opinion about an individual's: (i) racial or ethnic origin or (ii) political opinions; or (iii) membership of a political association; or (iv) religious beliefs or affiliations; or (v) philosophical beliefs; or (vi) membership of a professional or trade association; or (vii) membership of a trade union; or (viii) sexual orientation or practices; or (ix) criminal record; that is also personal information; or (b) health information about an individual; or (c) genetic information about a person that is not otherwise health information; or (d) biometric information that is to be used for the purpose of automated biometric verification or biometric identification; or (e) Biometric templates.'[27]
System of reliance	An ability to rely on identity commencement and assurance activities undertaken by another organisation (or area of an organisation) to authenticate a person's identity
Trusted biometrics	Biometrics collected electronically, using encrypted chip technology, from a machine-readable biometric passport, or travel document, issued by an accepted authority, captured to an agreed standard in a reputable process
Watchlist	A list of individuals, groups, or items that require close surveillance, typically for risk-based or legal reasons

27. As set out in Section 6 of the *Privacy Act 1988*